

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 September 2002 (06.09.2002)

PCT

(10) International Publication Number
WO 02/069656 A2

(51) International Patent Classification⁷: **H04Q 7/34**

(21) International Application Number: **PCT/EP02/00327**

(22) International Filing Date: **10 January 2002 (10.01.2002)**

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:
P101A000002 12 January 2001 (12.01.2001) IT

(71) Applicant (for all designated States except US): **SIMTEL S.R.L. [IT/IT]; Via Bonifacio Lupi, 25, I-50129 Firenze (IT).**

(72) Inventor; and

(75) Inventor/Applicant (for US only): **ANDREINI, Enrico [IT/IT]; Via Ugo Corsi, 19, I-50141 Firenze (IT).**

(74) Agent: **CIOPI, Gianluigi; Italbrevetti di G. Giorgi, Piazza della Libertà, 14, I-56025 Pontedera (IT).**

(81) Designated States (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.**

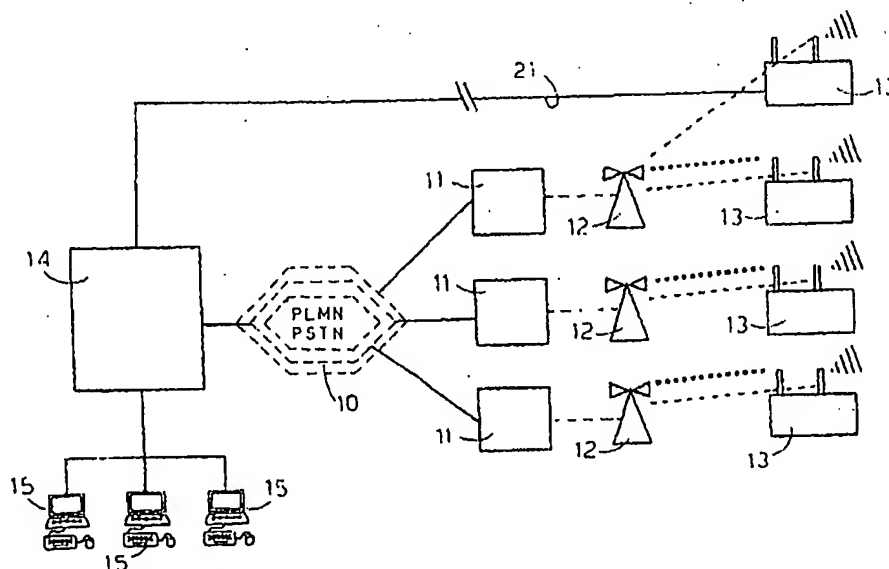
(84) Designated States (regional): **ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).**

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: **APPARATUS AND METHOD FOR VERIFYING ACCESS PROCEDURE TO MOBILE TELEPHONY NETWORKS THROUGH SIM CARDS**



(57) Abstract: An apparatus, and corresponding method, for verifying the procedure to access mobile telephony networks through SIM cards provides that said cards are stably placed in a single central electronic unit which, upon verification requests carried on by various phone service suppliers from remote terminals, is apt to read the parameters of the peripheral devices placed at the mobile telephony network area locations that are requested to be tested; in this way said devices act, in the various tests, as mobile telephones containing the specific SIM cards involved in the verifications. Data relating to verifications as well as said parameters are transmitted between peripheral devices and central electronic unit through dedicated digital transmission lines or through the telephony network itself.

APPARATUS AND METHOD FOR VERIFYING ACCESS
PROCEDURE TO MOBILE TELEPHONY NETWORKS
THROUGH SIM CARDS

o o o o o o o

FIELD OF THE INVENTION

The present invention concerns an apparatus, and corresponding method, for verifying the procedure to access mobile telephony networks through SIM cards.

DESCRIPTION OF THE PRIOR ART

The great part of the telephones radio-connected to peripheral stations of mobile telephony networks operate, as known, using SIM (Subscriber Identity Module) cards inserted in the telephone sets.

A card is activated by a certain phone service supplier at the moment in which a user asks for the telephonic service offered by that supplier; a new card is so inscribed to a new user.

To enlarge as much as possible the coverage of the service, even beyond the limits of the network area directly managed by the phone service supplier, sub-supply agreements take place between the various phone service suppliers in order to avoid drawbacks or

limitations for the users.

When, that is, a certain user of a mobile telephony network leaves an area where the telephony network of a first phone service supplier operates and enters an area where said network does not operate and a second supplier's telephony network operates, an authentication procedure starts in blind mode. By this procedure, substantially, it is detected if the user's card belongs to a telephone service supplier which has an agreement with the above second supplier; then, connecting to the first telephone service supplier, it is verified that the user is enabled to access the service, and, finally, the technical parameters needed to handle the communications, instead of the first supplier, are acquired.

It is evident to everyone how appropriately each phone service supplier has to verify the above procedure to work efficiently inside his own network area, not only when he activates the sub-supply of the service, but carefully and often, during the providing of the above sub-supply service, from the most locations available in the managed area, according to the different available kinds of connections, and whatever could be the communication type (voice message, alphanumeric message, data transmission, or other possible kind of transmission or required services).

At the present time the above verification is done, as regards each

service supplier which the first supplier has an agreement with, by placing the relating sample card in a mobile telephone and performing verification calls from various locations in the managed area.

Since each service supplier emits, for obvious reasons, the least needed amount of sample cards, generally one single card for each supplier which he has an agreement with, we can easily infer that said verifications are extremely slow and troubled, not as much due to their complexity as to the logistic problems which come from the above limitation.

SUMMARY OF THE INVENTION

Main aim of this invention is to propose an apparatus, and corresponding method, for verifying the procedure to access mobile telephony networks through SIM cards overcoming the limitation of low availability of cards itself and the need of placing them at the various locations of the managed network area.

Another aim of this invention is to propose a tester apparatus for verifying the procedure to access the network, which could perform various verifications from whatever location in the geographic area where a specific mobile telephony network operates, even if there are no stable data transmission instruments or lines and whatever the required service should be.

A further aim of this invention is to propose a verification system for

verifying the procedure to access mobile telephony networks which could automatically perform said verifications and these ones, furthermore, could be required by telematic lines.

Such aims are attained through an apparatus for verifying the procedure to access mobile telephony networks through SIM cards, comprising a central electronic unit, where SIM cards on which to execute the verifications are stably placed, and peripheral devices, connected, by means of dedicated telematic lines or by telephony networks, to said central unit which, upon verification requests carried on through remote terminals, reads initial parameters stored in said cards involved in the verification and transmits said parameters to said peripheral devices placed at the locations of the mobile telephony network specified in the verification request, said peripheral devices working, upon reception of said parameters, as mobile telephones containing the specific cards whose parameters have been transmitted to them.

A method for verifying the procedure to access mobile telephony networks through SIM cards provides

- placing said SIM cards in a single central electronic unit,
- positioning specific devices at the locations of the mobile telephony network where verifications are required,
- reading, through said central electronic unit, the parameters of the

SIM cards on which to execute the verifications,
-transmitting said parameters to said specific peripheral devices,
-performing verifications of the accessing procedure through said peripheral devices, said devices working, upon reception of said parameters, as mobile telephones containing the specific SIM cards whose parameters have been transmitted to them.

The method of the invention advantageously provides transmission of the SIM cards' working parameters between said central electronic unit and said peripheral devices, according to two different phases: a first phase in which some specific parameters, useful to authenticate the cards, are transmitted before verification, a second phase in which, during the verification, the remaining parameters, needed to complete authentication and to ensure normal working of cards and devices, are transmitted.

In this way, as we will see, we can use the mobile telephony network to transmit parameters stored in the SIM cards on which to execute the verifications, so we are free of positioning the peripheral devices for verification performing in whatever location of the geographic area where a certain mobile telephony network operates.

Another advantageous feature is the possibility of performing verifications without having to bring the SIM cards to the various locations of the managed telephony network, but just requesting the

verifications by telematic lines, so clearly saving time and resources, and even getting automatic production of verifications databases, helpful for later queries and checking activities.

Further advantages come from the effectiveness of the verifications, which can be automatically performed whenever desired.

BRIEF DESCRIPTION OF THE DRAWINGS

However, for a better understanding of the above-mentioned advantages and characteristics of the present invention, this will now be described by way of an embodiment example, with reference to the accompanying drawings, in which:

- figure 1 schematically shows the arrangement of the components of an apparatus according to the present invention in an integrated set of public land mobile networks and public switching telephony networks;
- figure 2 shows a block diagram of one of the components of the apparatus of fig.1;
- figure 3 shows a flow chart of the steps of a method according to the present invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

Referring first to fig.1, there is, very schematically shown, a whole, 10, of telephony networks which could be both public switching telephony networks (PSTN) and public land mobile networks

(PLMN), usually interacting between themselves. Switching stations of said whole 10, are referred as 11; they interface the mobile telephony networks and the fixed telephony networks, and are named Mobile Switching Center (MSC).

From these MSC, 11, the mobile telephony networks branch out. In fig.1 just the terminal stations, 12, of said networks are shown, for the simplicity of the representation. Said terminal stations are named Base Transmitting Stations (BTS) and, as known, constitute the core of the cells, or geographic areas, which compose the zone covered by a mobile telephony network.

In the above general scheme, peripheral devices for verifying the procedure to access mobile telephony networks through SIM cards are referred as 13.

Said devices comprise, as better seen in the following, two radio transmitting and receiving units, or, alternatively, one unit apt to transmit and receive via radio and one unit apt to transmit and receive through dedicated digital lines.

The general scheme of fig.1 is completed with a central electronic unit, 14, which is apt to:

- house all the SIM cards on which to execute the verifications,
- read the parameters stored in said cards,
- transmit said parameters and the instructions for performing the

verifications to the peripheral devices, 13,

- receive from these ones said parameters suitably updated upon verifications,
- store the updated parameters in the SIM cards housed in it, and, finally,
- receive and store results of the verifications performed by the peripheral devices.

All the above happens upon verification requests which come to said central electronic unit through remote terminals, 15, connected to it and generally associated to the phone service suppliers of the various networks, which have sub-service agreements between them.

Peripheral devices, 13, are constituted, as we can see in the block diagram of fig.2, of a microcomputer unit, 16, and two modules, 17 and 18, which are the radio units of two mobile telephones. Each of said modules comprises whichever base function of a standard mobile telephone but doesn't comprise the user interfaces, such as keyboard, display, microphone and receiver.

In particular, one of said modules, 17, has a resident SIM card, as usually occurs in a standard mobile telephone, while the other module, 18, is connected to a memory unit, 20, which simulates the SIM card on which to execute the verifications, housed in the central electronic unit, 14. Said memory unit, 20, so acts as a virtual SIM card for

module, 18.

The above described apparatus operates as follows.

Upon a specific verification request got to central electronic unit, 14, through one of the remote terminals, 15, said central unit performs a reading of the authentication parameters, such as IMSI, TMSI, or similars, stored in the SIM card on which to execute the verification, and transmits, both said parameters and instructions for executing the verification, to the device, 13, stated in the verification request. It has to be noticed that the above data are transmitted to the CPU, 16, or through dedicated digital lines, 21, other through the mobile telephony network by using module, 17, equipped with its own SIM card, 19.

CPU, 16, stores the above mentioned authentication parameters in the memory unit, 20, which module, 18, interfaces with during the verification. The verification start up time and the telephone number to dial for performing the verification are stored in the RAM unit, 22, of the CPU, 16.

So, this last one, at the fixed time, sends to module, 18, the data concerning the telephone number to dial, in order to begin the calling as it would happen if an operator dials the number by the keyboard of a mobile telephone including the SIM on which to execute the verification.

Once the calling has begun, module, 18, reads on the virtual card, 20, the parameters needed to start the authentication procedure; then it sends the access request, through the mobile telephony network, to the supplier which emitted the SIM card under verification; said supplier launches the authentication procedure for that specific card by sending to module, 18, some variables, RAND, which the SIM card under verification has to process according to a specific algorithm, stored in it.

To do this, CPU 16, transmits said variables, RAND, through module, 17, to the central electronic unit, 14, which, as above said, houses the specific SIM card storing the above specific authentication algorithm that, for secrecy reasons, could not be transmitted to the virtual card, 20, together with the other parameters previously transmitted from central electronic unit, 14, to peripheral device, 13.

Once RAND variables have been processed, the processing output, consisted of SRES (Signature Response) parameter, is transmitted from SIM card under verification to module, 18, still through the central electronic unit, 14, and through the auxiliary module, 17, which are to one another connected through the mobile telephony network.

Together with said SRES parameter is also transmitted the KC (Key Cyphering) parameter, since module 18, once the SRES parameter has been verified to be the right one, sends said KC parameter to the SIM

card manager to get the code needed to support the conversation; note that, in this embodiment of the invention, conversation represents the required type of phone communication among the available kinds of transmissions and services.

Finally, as last step before the conversation, module 18, just like whichever mobile phone would do while regularly working, asks to the service supplier, through the standard mobile telephony network, for the assignment, that is the right of managing the phone connection.

Once obtained said assignment, module 18 transmits a predefined vocal message, then, got the relating answer, shuts down the connection and updates the parameters stored in the virtual card 20.

The CPU unit, 16, of device, 13, reads, from the virtual card, 20, said updated parameters and transmits them to the SIM card housed in the central unit, 14, by means of the digital line, 21, or of the standard telephony network, using, in this second case, the module 17 of the device 13 itself.

All the above is schematically condensed in the flow chart of fig.3, where the three different "areas" or physically separated units which exchange data during the verification procedure are pointed out.

Said pointing out is helpful to understand that the apparatus, and corresponding method, proposed with the present invention, allows

to verify the procedure to access the network from whichever location on the network area without the requirement that SIM cards on which to execute the verifications be physically available at said locations. This is possible since, by the method of the invention, the only moment in which, during verification, access to the SIM card is required is when authentication parameters have to be processed through the card's own algorithm; and, by the method of the invention, the above access occurs upon phone connection between module 17 and central electronic unit 14 housing the card, phone connection which takes a few time that, anyway, in that specific phase of the authentication procedure, the procedure itself allows, as it happens every time a mobile telephone dials a calling.

The other moment in which, during an authentication procedure, access to the card is required is that one useful for acquiring the initial parameters, just after dialling; to do this the time amount allowed in a standard procedure is not enough to perform the acquisition through a phone connection. This problem is solved, as seen, by the apparatus of the invention, with the help of the virtual card, 20, where said initial parameters are stored before performing verification procedure and they are simply read from module 18, that thus employs the same time amount needed if the SIM card on which to execute the verification would be physically placed at the location of the

verification.

Obviously the above limitations related to the connection time for acquiring whichever parameter needed during the authentication procedure do not exist if connection between central electronic unit, 14, and peripheral devices, 13, takes place through dedicated digital lines, 21; in fact, using this kind of lines, highly increased transmission speed, with respect to the radio transmission, can be reached. It has to be noted that, in this case, peripheral devices, 13, could be simplified since module, 17, radio transmitting and receiving, is no more needed, but, of course, with this solution the effectiveness and flexibility of the system would strongly decrease, because said devices could not be located wherever in the network area, but just where a telematic connection exists.

However, this last version of the peripheral devices may be provided and adopted, instead of the ones made according to the scheme of fig.2, in the locations of the network area where we can find digital lines such as TCP/IP or similar. In this case, the general advantages of the invention, represented by the capacity of automatically verifying the procedure to access the network through SIM cards even if said cards are not physically placed at the points of the network where verification is requested, are still safe.

Obviously further modifications and embodiments, different from the ones above shown as examples, can be provided generally considering that the most effectiveness of the apparatus and method of the invention is attained when peripheral devices 13 are apt to allow

acquisition of the SIM card's parameters through phone connection.

The modifications may be carried out, anyway, within the limits of the invention as defined by the following claims.

CLAIMS

1- Apparatus for verifying the procedure to access mobile telephony networks through SIM cards, comprising
a central electronic unit (14) where SIM cards on which to execute the verifications are stably placed,
peripheral devices (13), connected, by means of dedicated telematic lines (21) or by telephony networks, to said central electronic unit, wherein, said central electronic unit provides means for, upon a verification request carried on through remote or local terminal (15), reading parameters stored in the SIM card specified in said verification request, or processed according to algorithms stored in said SIM card, means for transmitting said parameters to the peripheral devices (13) placed at the locations of the mobile telephony network specified in said verification request, and,
said peripheral devices provide means for working, upon reception of said parameters, as mobile telephones containing the specified SIM cards whose parameters have been transmitted to them.

2- Apparatus according to claim 1 wherein said peripheral devices (13) comprise a first module (17) and a second module (18), both receiving and transmitting through mobile telephony networks, said first module being equipped with a resident SIM card (19), said second module lacking a SIM card but being connected to a memory

unit (20) operating as a virtual SIM card, a microcomputer unit (16) which can be connected to said central electronic unit (14) through dedicated telematic line (21) or through said first module (17), said unit (16) providing means for:

- receiving from said central electronic unit (14) data for performing verifications and parameters of the SIM card, specified in the verification request, housed in said central electronic unit,
- storing parameters of said SIM card in said memory unit (20),
- controlling, according to received data, said second module (18) for performing test callings and said first module (17) for performing auxiliary callings useful for acquiring and transmitting working SIM cards parameters,
- transmitting to said central electronic unit (14) the results of the verifications and the updated parameters of the SIM card specified in the verification request.

3- Apparatus according to claim 1 wherein said peripheral devices (13) comprise a module (18) transmitting and receiving through mobile telephony networks, said module lacking a SIM card but being connected to a memory unit (20) operating as a virtual SIM card, a microcomputer unit (16) which can be connected to said central electronic unit (14) through digital telematic line (21), said unit (16) providing means for:

- receiving from said central electronic unit (14) data for performing verifications and parameters of the SIM card, specified in the verification request, housed in said central electronic unit,
- storing parameters of said SIM card in said memory unit (20),
- controlling, according to received data, said module (18) for performing test callings,
- transmitting to said central electronic unit (14) the results of the verifications and the updated parameters of the SIM card on which the verification has been executed.

4- Method for verifying the procedure to access mobile telephony networks through SIM cards, comprising the steps of:

- housing the SIM cards on which to execute the verifications in a single central electronic unit (14);
- locating specific devices (13) at the points of the mobile telephony network where verifications are required, said peripheral devices being able to be connected to said central electronic unit through dedicated telematic lines (21) either through telephony networks;
- receiving, by said central electronic unit, requests of verification of the procedure to access the network through specific SIM cards housed in said central unit, said requests being carried out through remote or local terminals (15) connected to said central unit (14);
- transmitting data concerning the verifications to be executed, the

transmission occurring from said central unit (14) towards the peripheral devices (13) stated in the verification requests;

- starting, by said peripheral devices, the verifications according to the received data and, at the same time, requiring specific parameters stored or processed according to algorithms stored in said specific SIM cards housed in said central unit (14);

- transmitting, from said central unit (14) to said peripheral devices (13), parameters stored or processed according to algorithms stored in said specific SIM cards;

- completing, by said peripheral devices, the verifications of the procedure to access the network, said devices acting, upon reception of the above parameters, as mobile telephones containing the specific SIM cards whose parameters have been transmitted to them;

- transmitting the results of the verifications and the updated parameters of the SIM cards involved in the verifications to said central electronic unit (14) for storing said results and updating the parameters stored in said SIM cards housed in said central unit.

- 5- Method for verifying the procedure to access mobile telephony networks through SIM cards, comprising the steps of:

- housing the SIM cards on which to execute the verifications in a single central electronic unit (14);

- locating specific devices (13) at the points of the mobile telephony

network where verifications are required, said peripheral devices being able to be connected to said central electronic unit through fixed or mobile telephony networks;

-receiving, by said central electronic unit, requests of verification of the procedure to access the network through specific SIM cards housed in said central unit, said requests being carried out through remote or local terminals (15) connected to said central unit (14);

-transmitting data concerning the verifications to be executed and specific initial parameters stored in said specific SIM cards, the transmission occurring from said central unit (14) towards the peripheral devices (13) stated in the verification requests;

-starting, by said peripheral devices, the verifications according to the received data and, at the same time, requiring further parameters processed according to algorithms stored in said specific SIM cards housed in said central unit (14);

-transmitting, from said central unit (14) to said peripheral devices (13), parameters processed according to algorithms stored in said specific SIM cards;

-completing, by said peripheral devices, the verifications of the procedure to access the network, said devices acting, upon reception of the above parameters, as mobile telephones containing the specific SIM cards whose parameters have been transmitted to them;

-transmitting the results of the verifications and the updated parameters of the SIM cards involved in the verifications to said central electronic unit (14) for storing said results and updating the parameters stored in said SIM cards housed in said central unit.

6- Method for verifying the procedure to access mobile telephony networks through SIM cards according to claim 4 or 5, wherein said transmission of data concerning the verifications to execute and of data concerning stored or processed parameters, from said central electronic unit (14) toward said peripheral devices (13), takes place by employing a first module (17), apt to transmit and receive through mobile telephony networks, included in said peripheral devices (13), and wherein said verifications execution takes place by employing a second module (18), apt to transmit and receive through mobile telephony networks, included in said peripheral devices (13), said first module (17) being equipped with a resident SIM card (19), said second module (18) lacking a SIM card but being connected to a memory unit (20) operating as a virtual SIM card.

1/2

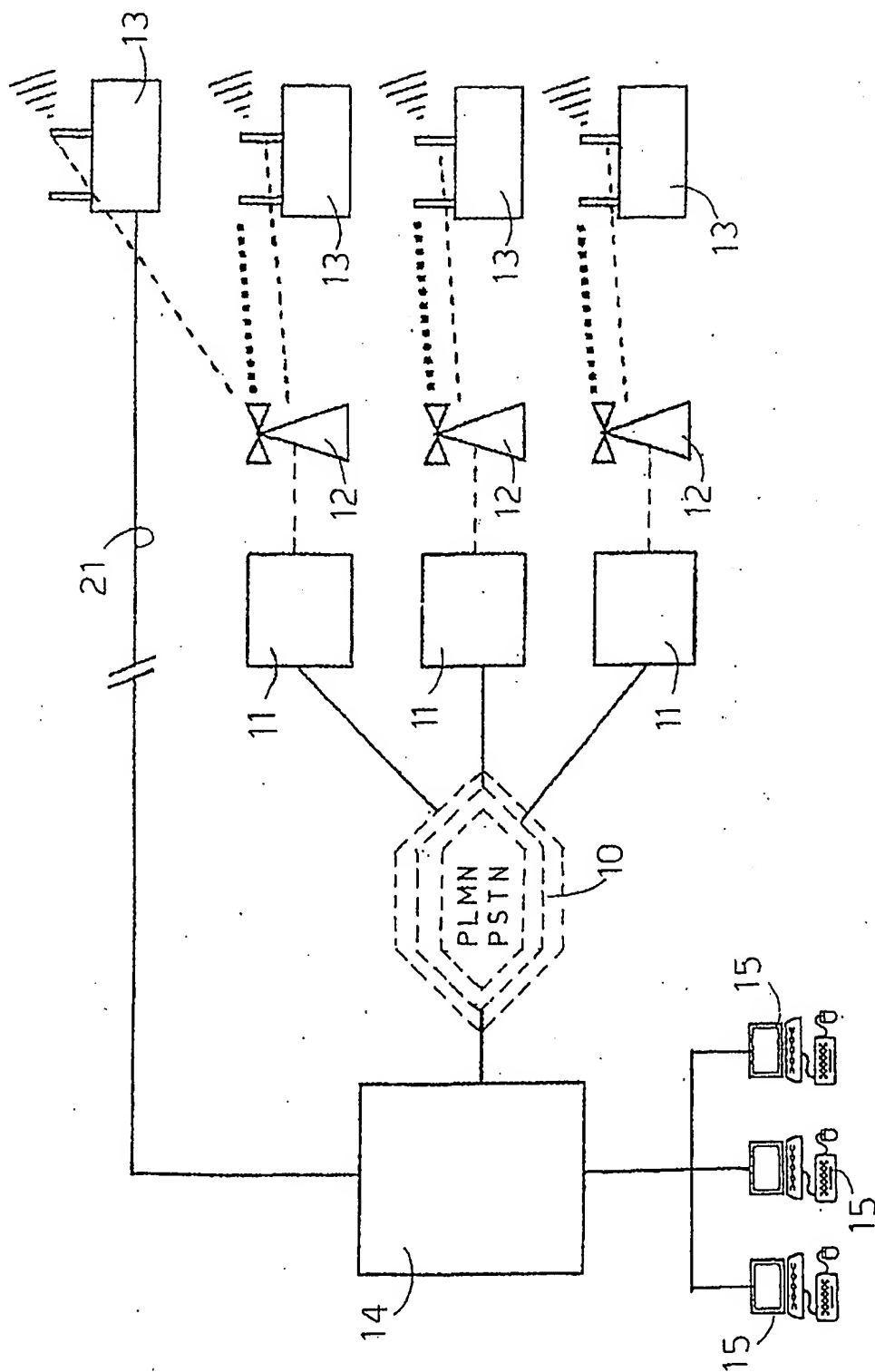


FIG. 1

2/2

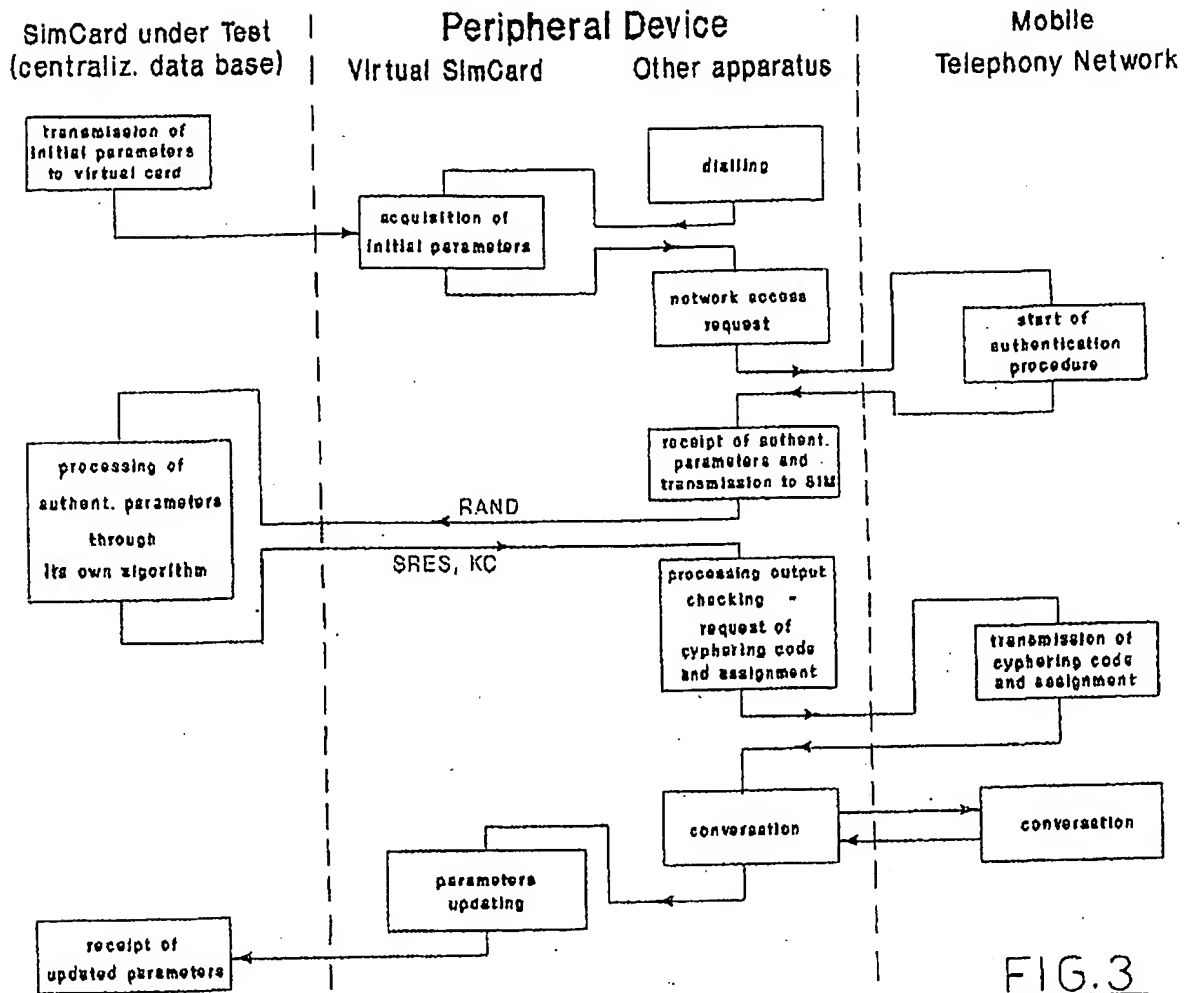


FIG.3

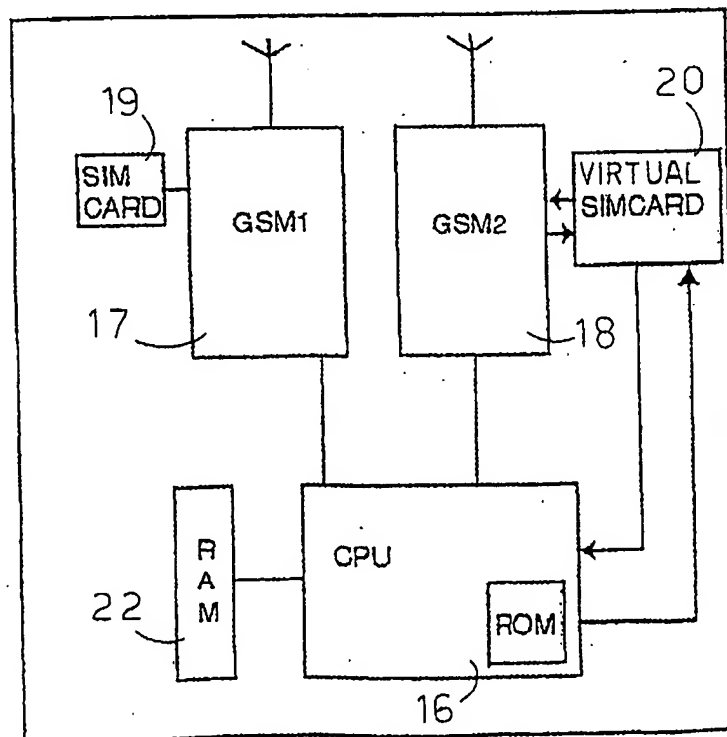


FIG.2